Technical Cybersecurity

Cain & Abel

Swiss Army Scanner

ORIGINALLY A PASSWORD CRACKER

‣ Created by Massimiliano Montoro, first released in 2003

‣ Added algorithms

‣ Added functionality (ARP attacks, network sniffing)

‣ Windows only

Large Number of Algorithms

WINDOWS ALGORITHMS

- ‣ LANMAN, NT, NTLM, Kerberos
- ‣ Supports various passing protocols
  - ‣ SMB, IMAP, POP, SMTP, NNTP, etc.

OTHER ALGORITHMS

- ‣ Cisco IOS/PIX
- ‣ RADIUS
- ‣ IKE
- ‣ and more

Sniffing Traffic

VARIETY OF NETWORK PROTOCOLS

‣ FTP, Telnet, SMTP, HTTP, IMAP, POP3, VNC, TDP, MySQL, MS SQL, SMB, SIP/RTP, HTTPS (via MitM), SSHv1 (via MitM)

ARP SPOOFING

‣ Similar to Ettercap/Bettercap

‣ Route traffic through Cain, steal passwords en-route

Next up, technical details on what some of these things are.